

**IN THE UNITED STATES DISTRICT COURT FOR THE
EASTERN DISTRICT OF VIRGINIA**

Alexandria Division

UNITED STATES OF AMERICA)	
)	
v.)	Criminal No. 1:19-CR-304 (LMB)
)	
HENRY KYLE FRESE,)	
)	
Defendant)	

GOVERNMENT’S POSITION WITH RESPECT TO SENTENCING

The United States, by and through its undersigned counsel, hereby files its position on sentencing. The United States has no objections or corrections to the presentence report (“PSR”). While the U.S. Sentencing Guidelines (“USSG”) calculation is 120 months, based on the information in the government’s sealed filing and application of the 18 U.S.C. § 3553(a) sentencing factors, the government asks that the Court sentence the Defendant Henry Kyle Frese (the “defendant”) to 108 months’ imprisonment. For the reasons stated below, a nine-year sentence is commensurate with the defendant’s betrayal in this case. The defendant betrayed the oath he took to the United States to protect classified national defense information (“NDI”). He did so by passing SECRET and TOP SECRET national defense information to two journalists and an overseas consultant on at least 19 separate occasions. He did so for his own selfish interests. A nine-year sentence furthers the interests of justice in this case and further serves to protect the national security of the United States.

I. PROCEDURAL HISTORY

On October 8, 2019, a grand jury sitting in the Eastern District of Virginia returned an indictment charging Henry Kyle Frese, who was then employed as a Defense Intelligence Agency (“DIA”) analyst, with two counts of willful transmission of NDI in violation of 18 U.S.C. § 793(d). On February 20, 2020, the defendant appeared before this Court and entered a plea of guilty to Count One of the Indictment. Sentencing is currently scheduled for June 18, 2020.

II. FACTUAL HISTORY

The defendant began working for DIA as a contractor in January 2017. *See* Statement of Facts (“SOF”), ¶ 2 [Dkt. 42]. In order to work as a contractor at DIA, the defendant maintained a TOP SECRET//SCI¹ U.S. government security clearance and had access to NDI classified up to the TOP SECRET//SCI level. *Id.*; *see also* Presentence Investigative Report (“PSR”) at ¶ 9 [Dkt. 46]. In 2018, the defendant became a full-time employee of DIA, maintaining his TOP SECRET//SCI security clearance and access to classified NDI. SOF at ¶ 2; PSR at ¶ 9. For both his contractor role and his subsequent full-time employment with DIA, the defendant underwent training in the proper handling of classified NDI and the potential damage to the United States from the unauthorized disclosure of classified information. SOF at ¶ 6; PSR at ¶ 13.

From January 2018 until November 2018, the defendant lived with a certain journalist (“Journalist 1”). SOF at ¶ 10; PSR at ¶ 17. The defendant and Journalist 1 followed each other on Twitter, meaning each could see what the other was posting on that platform. SOF at ¶ 11; PSR at 18. While the defendant was living with Journalist 1, she published eight articles containing

¹ Access to SCI is further restricted beyond the restrictions already in place for classified information. SCI is a type of classified information concerning or derived from sensitive intelligence sources, methods, or analytical processes. SCI must be handled within formal access control systems established by the Director of National Intelligence. One must receive explicit permission to access an SCI control system or compartment. Once it is determined a person should have access to an SCI compartment, that person signs a nondisclosure agreement specific to that compartment.

classified NDI related to certain foreign countries' weapons capabilities. SOF at ¶ 8; PSR at 15.

On one particular occasion related to Journalist 1's reporting on these foreign countries' weapons capabilities, Journalist 1's publication ("Article 1") came almost immediately after the defendant spoke with both Journalist 1 and a second journalist ("Journalist 2") who worked for a media outlet affiliated with the one for which Journalist 1 worked. SOF at ¶ 16; PSR at ¶ 23. Prior to the publication of Article 1, the defendant had viewed on multiple occasions an intelligence product containing the same NDI subsequently published in Article 1 ("Intelligence Product 1"). SOF at ¶ 14; PSR at 21. After his second viewing of Intelligence Product 1, in April 2018, the defendant and Journalist 1 exchanged direct messages on Twitter discussing Journalist 2's attempt to verify with a high level government official information the defendant had provided from Intelligence Report 1. *Id.* at ¶ 15; PSR at 22; *see also* Redacted April 2018 Twitter Exchange² (Ex. A). Twice during the conversation, the defendant characterized the government denial as "weird" based on the information he had seen in Intelligence Report 1. *See* Redacted Twitter Exchange at 2-3.

Journalist 1 raised the idea of introducing the defendant to Journalist 2 during the same April 2018 Twitter conversation. *Id.* at 3. Journalist 1 asked if the defendant would be willing to speak with Journalist 2 on a certain topic. *Id.* The defendant responded to Journalist 1 that "[i]f helping her helps you, I'm down. I just want to see my bubs progress." *Id.*

Following the April 2018 Twitter exchange, the defendant ran search terms related to the topic of Intelligence Report 1 on a classified government computer system. SOF at ¶ 16; PSR at ¶ 23. Several hours after running the searches, the defendant spoke with Journalist 1 for seven minutes. *Id.* A few hours after the call with Journalist 1, the defendant spoke with Journalist 2 for

² The unredacted Twitter exchange has been provided as Class'd Ex. 7 to Gov't Class'd Add.

over half an hour, before again speaking briefly with Journalist 1. *Id.* Half an hour after the back-to-back calls with both journalists, Journalist 1 published Article 1. *Id.* After publication of Article 1, Journalist 1 posted a Tweet with a link to the article. SOF at ¶ 17; PSR at ¶ 24. The defendant then “retweeted” Journalist 1’s Tweet, meaning he posted the content, including the link to the article containing classified NDI, to his own Twitter feed. *Id.*

On September 24, 2019, the defendant sent a text to Journalist 2 stating, “Hi hi. If you’ve got time give me a call, otherwise we can chat tomorrow! I know it’s late, sorry!” *See* Sept. 24, 2019 Text Message (Ex. B). During a subsequent telephone call between the defendant and Journalist 2, recorded pursuant to court authorized Title III monitoring of the defendant’s mobile phone, the defendant brought up a topic the pair had not previously discussed:

Journalist 2: Um, what’s going on at work?

Defendant: Uh, well it’s nothing to do with, like what I cover, per usual but um, it’s, so it’s about, still like [Intelligence Report 2 & 3].

[. . .]

Defendant: I don’t know if that would be of interest to you but I thought . . .

Journalist 2: It’s definitely of interest[.]

See Redacted Transcript of Sept. 24, 2019 Telephone Call³ (“Redacted Sept. 24 Call. Tr.”) at 2 (Ex. C). The defendant then proceeded to disclose NDI classified at the SECRET level to Journalist 2 during their phone conversation. *See* Unredacted Transcript of Sept. 24, 2019 Telephone Call (Class’d Ex. 8 to Class’d Gov’t Add.); Classified Recording of Sept. 24, 2019 Call (Class’d Ex. 8a).

³ A classified unredacted version of the transcript, along with an audio recording of the call, have been provided to the Court and defense counsel as Classified Exhibits 8 and 8a to the Government’s Classified Addendum.

Between March 1, 2018, and October 8, 2019, the defendant spoke with Journalist 1 by telephone at least 630 times and the pair exchanged at least 57 text messages. SOF at ¶ 22; PSR ¶29. From mid-2018 to late September 2019, the defendant orally transmitted TOP SECRET NDI to Journalist 1 on at least 12 separate occasions. SOF at ¶ 13; PSR at ¶ 20. During the same time period, he orally transmitted SECRET NDI to Journalist 1 at least four times. *Id.* Between mid-2018 and October 2019, on at least two separate occasions, the defendant confirmed the accuracy of NDI classified at the SECRET and TOP SECRET levels that someone else had previously provided to Journalist 1. SOF at ¶ 20; PSR at ¶ 27. In addition to passing and confirming the accuracy of NDI, the defendant conducted searches on classified government computer systems regarding topics he discussed with Journalist 1 and Journalist 2 on at least 30 separate occasions throughout 2018. SOF at ¶ 18; PSR at ¶ 25. Some of those searches were outside the scope of the defendant's job responsibilities and conducted in response to a specific request for information from one of the journalists. SOF at ¶ 19; PSR at ¶ 26. Throughout the time the defendant was passing NDI, confirming the accuracy of NDI passed by others, and running targeted searches at the journalists' behest, he knew he was not authorized to share classified information with either journalist. SOF at ¶ 24; PSR at ¶ 31.

Separate and apart from the defendant's illegal disclosures of classified NDI to members of the media, the defendant was also passing classified NDI to a foreign consultant ("Consultant 1"). *See* SOF at ¶ 25; PSR at ¶ 32. Consultant 1 worked for an overseas consulting group focused on counterterrorism issues. *Id.* On at least two occasions, the defendant transmitted classified NDI to Consultant 1, knowing that he was not authorized to transmit NDI to Consultant 1. SOF at ¶¶ 25-26; PSR at ¶¶ 32-33.

III. APPLICABLE LAW AND GUIDELINES CALCULATION

The advisory guidelines range, as calculated pursuant to the USSG is not binding upon the Court and instead constitutes a “starting point and initial benchmark” in the sentencing analysis. *Gall v. United States*, 552 U.S. 38, 49-50 (2007). Nonetheless, “a court of appeals may apply a presumption of reasonableness to a sentence imposed by a district court within a properly calculated guideline range” USSG Manual, published November 1, 2018, at 14 (citing *Rita v. United States*, 551 U.S. 338 (2007)). After ensuring that the advisory guideline range is properly calculated, the Court must consider whether a sentence within that range serves the factors and purposes set forth in 18 U.S.C. § 3553(a). *See United States v. Moreland*, 437 F.3d 424, 432 (4th Cir. 2006). If it does not, the Court must determine whether grounds for a departure exist under the guidelines or pertinent case law and apply them, as appropriate. *Id.*; *see also United States v. Tucker*, 473 F.3d 556, 560-61 (4th Cir. 2007) (consider departure ground before imposing variance). If, following that analysis, the Court still deems a sentence within the advisory guidelines range to be inadequate, the Court may further vary, above or below, that advisory range until it reaches a sentence that best serves the statutory sentencing factors and purposes. *See Moreland*, 437 F.3d at 432. Finally, the Court must state its reasons for imposing such a sentence, taking care to explain the reasons for any departure or variance. *Id.*; *see also* 18 U.S.C. § 3553(c)(2).

In this case, the probation officer and the government agree that the sentencing guidelines recommend a sentence of 120 months’ imprisonment. *See* PSR at ¶ 87. The base offense level of 35 is based on the defendant’s conviction for the oral, willful transmission of TOP SECRET NDI, in violation of Title 18, United States Code, Section 793(d). USSG § 2M3.1; *see also* Plea Agreement at 4.a. [Dkt. 41]. With a two-level decrease for acceptance of responsibility (USSG §

3E1.1(a)) and a two-level increase for abuse of a position of trust (USSG § 3B1.3), the resulting offense level is 35. Based on the defendant's assistance "in the investigation [and] prosecution of his own misconduct by timely notifying authorities of his intention to enter a plea of guilty," the government hereby moves this Court for an additional one level decrease. *See* USSG § 3E1.1(b). With the additional one-level reduction, the defendant's base offense level is 34. The defendant has no prior criminal history, resulting in a Criminal History Category of I. The associated sentencing guidelines range is 151-188 months, well above the statutory cap of 120 months for the offense of conviction.

The defendant does not dispute that the abuse of position of trust enhancement applies here. *See* Plea Agreement ¶ 4.a. [Dkt. 41]. The defendant used information he obtained while working in a sensitive government position. Courts in this district and the Fourth Circuit have previously applied the abuse of position of trust enhancement in similar circumstances. *United States v. Ford*, 288 F. App'x. 54, 61 (4th Cir. 2008) (finding no error in application of abuse of position of trust enhancement for 18 U.S.C. § 793 conviction because defendant's "abuse of his position of public trust contributed significantly to his commission of the offense. [The defendant] simply would not have been able to commit the offense of retaining classified documents without permission if he had not held a top secret security clearance. . . ."); *United States v. Mallory*, Case No. 1:17-cr-154, Dkt. 280, at 16 (E.D. Va. July 30, 2019) (Ellis, J.) ("He only retained the information because of the position of trust that he held at the time that he was employed by the agency."); *United States v. Pitts*, 973 F. Supp. 576, 584 (E.D. Va. 1997) (Ellis, J.) (increasing abuse of position of trust enhancement by one additional level for former FBI agent convicted of violating 18 U.S.C. § 794 who "held a special position of awesome responsibility and trust [and] was supposed to safeguard this nation from foreign espionage activity" but who "[i]nstead . . . betrayed his country by

engaging in the very activity that he was sworn to protect the nation against”), *aff’d*, 176 F.3d 239, 245 (4th Cir. 1999) (affirming district court’s enhancement where “abuse of trust was extraordinary”); *see also United States v. Albury*, Case No. 0:18-CR-67, Dkt. 58, at 14 (“The abuse of trust adjustment reflects that [the defendant] used his position as an FBI agent and his security clearance to facilitate the crime in a significant way.”); *United States v. Winner*, Case No.1:17-34, Dkt. 324, at 7 (S.D. Ga. Aug. 23, 2018) (agreement by both parties as to applicability of abuse of position of trust enhancement in media leak case charging violation of 18 U.S.C. § 793(e)).

Here, the guidelines calculation of 151-188 months exceeds the statutory maximum penalty for 18 U.S.C. § 793(d) of 10 years’ imprisonment. Thus, the USSG calculation for the defendant is the statutory maximum of 120 months. *See* USSG § 5G1.1(a). Based on the further information in the government’s sealed filing, and application of the 18 U.S.C. § 3553(a) factors below, a sentence of 108 months—nine years—is appropriate here.

IV. A 108-MONTH SENTENCE IS APPROPRIATE

B. 18 U.S.C. § 3553(a) Factors Support a 108-Month Sentence

In addition to the sentencing guidelines range, the factors for the district court to consider at sentencing include: (1) the history and characteristics of the defendant; (2) the nature and circumstances of the offense; (3) the important need for the sentence to reflect the seriousness of the crime and deter future criminal conduct; and (4) the need to avoid unwarranted sentencing disparities. 18 U.S.C. § 3553(a).

1. History and Characteristics of the Defendant

The defendant is a 31-year-old former counterterrorism intelligence analyst. The defendant worked in the intelligence community for over three years, first as a cleared defense contractor and later as a full-time DIA intelligence analyst. The defendant was a sophisticated intelligence

professional, who had received extensive training in the proper handling of classified information. *See, e.g.*, SOF at ¶ 6; PSR at ¶ 13. Based on his training and work as an intelligence analyst, the defendant knew the potential harm to the national security that could result from the unauthorized disclosure of classified NDI. SOF at ¶¶ 6-7; PSR at ¶¶ 13-14. In particular, the defendant knew that the unauthorized disclosure of SECRET information had the potential to cause serious harm to the national security and that the unauthorized disclosure of TOP SECRET information had the potential to cause exceptionally grave damage to the national security. SOF at ¶ 6; PSR at ¶ 13. Despite this understanding, the defendant knowingly and repeatedly disclosed to multiple individuals, including two journalists, information that could be damaging to the United States and used to the advantage of this country's adversaries.

2. *Nature and Circumstances of the Offense*

The defendant's conduct was purposeful and ongoing. Over the course of an approximately 17-month period, the defendant transmitted classified NDI to members of the media at least 17 times, including at least 12 instances of passing NDI classified at the TOP SECRET level. SOF at ¶¶ 13, 21; PSR at ¶¶ 20, 28. Based on his training, the defendant knew that the unauthorized transmission of TOP SECRET information can reasonably be expected to cause exceptionally grave damage to the national security of the United States. *See* SOF at ¶¶ 3, 6; PSR at ¶¶ 10, 13. In addition, the defendant was, at times, confirming the accuracy of classified NDI Journalist 1 and Journalist 2 had learned elsewhere. SOF at ¶ 20; PSR at ¶ 27. Such confirmation as to the accuracy of classified government NDI is, in and of itself, a violation of the Espionage Act. *See, e.g., Alfred A. Knopf, Inc. v. Colby*, 509 F.2d 1362, 1370 (4th Cir. 1975) ("It is one thing for a reporter or author to speculate or guess that a thing may be so or even, quoting undisclosed sources, to say that it is so; it is quite another thing for one in a position to know of it officially to

say that it is so.”); *cf. Simmons v. U.S. Dep’t. of Justice*, 796 F.2d 709, 712 (4th Cir. 1986) (“[R]elease from an official source naturally confirms the accuracy of the previously leaked information and may damage the nation’s standing even when unofficial parties have previously disclosed the documents.”). Above and beyond passing to and confirming the accuracy of classified NDI for Journalist 1 and Journalist 2, the defendant further disseminated the unauthorized disclosures by re-Tweeting Journalist 1’s articles on Twitter. *See* SOF at ¶¶ 11, 17. Thus, the defendant further violated the trust placed in him as a clearance holder by assisting in disclosing the compromised NDI more broadly to both the American public and our adversaries worldwide.

The highly sensitive material the defendant was passing to the two journalists largely fell outside the scope of his job duties, much of it relating to the weapons capabilities of certain foreign countries. Thus, to facilitate the transfer of information that had the potential to do exceptionally grave damage to our nation’s security, the defendant was conducting searches on classified government systems—systems he only had access to due to the trust placed in him by his government as a clearance holder. In fact, on at least 30 separate occasions in 2018 alone, the defendant ran classified searches on the same topic about which Journalist 1 was writing during the same time period. *See* SOF at ¶¶ 16, 18; PSR at ¶¶ 23, 25. Even more troubling, the defendant admits that, at times, he used his special access to sensitive NDI to run classified searches at the specific behest of either Journalist 1 or Journalist 2. SOF at ¶ 19; PSR at ¶ 26. Records show that the defendant would sometimes leave his duty station in a Sensitive Compartmented Information Facility (“SCIF”) during work hours in order to call Journalist 1 and Journalist 2 to relay information he learned by searching classified government systems. *Cf.* SOF at ¶ 16; PSR at ¶ 23.

The defendant appears to have been motivated to betray the trust placed in him by this

country by a desire to help a journalist with whom he was romantically involved. *See, e.g.*, SOF at ¶ 15; PSR at ¶ 22. For example, during the April 2018 Twitter exchange with Journalist 1, when asked whether he would be willing to start engaging with Journalist 2, the defendant responded “[i]f helping her helps you, I’m down. I just want to see my bubs progress.” *See* April 2018 Twitter Exchange at 3 (Ex. A). Given the hybrid nature of the defendant’s relationship with Journalist 1 – both a source of NDI and a romantic interest – it is unsurprising that the defendant and Journalist 1 were in frequent contact. In fact, between March 1, 2018 and October 8, 2019, the defendant participated in at least 630 phone calls and exchanged at least 57 text messages with Journalist 1. SOF at ¶ 22; PSR at ¶ 29. As to Journalist 2, however, the defendant himself admits that their relationship was limited solely to discussion of topics Journalist 2 was investigating. SOF at ¶ 23; PSR at ¶ 30. Given this, the frequency of communications between the defendant and Journalist 2 is notable. Over the course of less than 17 months, the defendant and Journalist 2 exchanged at least 151 text messages and participated in at least 34 voice-to-voice calls.⁴ *Id.* Again, these 185 known communications between the defendant and Journalist 2 were solely for the purpose of discussing topics Journalist 2 was investigating for potential publication.

The government often notes in cases involving disclosure of classified NDI to the media that these cases are so harmful because the disclosure is not really made just to the media. When our nation’s secrets are published, in print or online, those secrets are made available to all of our adversaries. In fact, a foreign military officer from Russia confirmed as much when he wrote “I was amazed—and Moscow was very appreciative—at how many times I found very sensitive information in American newspapers. In my view, Americans tend to care more about scooping their competition

⁴ The defendant was speaking with Journalist 2 on not only her mobile telephone but also on at least two landlines associated with media outlets. Thus, it is possible Journalist 2 communicated with the defendant from other numbers of which the government is not aware in addition to these three referenced telephone lines.

than about national security, which made my job easier.” Stanislav Lunev, *Through the Eyes of the Enemy* 135 (Regnery Publishing, Inc.) (1998). Former Central Intelligence Agency (“CIA”) Director George Tenet confirmed the risk created by broad dissemination of our nation’s secrets:

I just need to reinforce that when you throw this [classified] information out, it often appears innocuous to someone who’s leaking information. That’s not the prism to look at it in. It’s the adversary’s counterintelligence. And his ability to put together the pieces of the puzzle that put at risk your human operations, your technical operations, your analytical products, and jeopardizes investment that we’ve made to protect the American people.

Hearing before the Senate Select Committee on Intelligence: Current and Projected National Security Threats to the United States, S. Hrg. 106–580, p. 158 (February 2, 2000).⁵ This sentiment was echoed a few years later by a subsequent CIA Director, Porter J. Goss, who also underscored the damage caused by leaks of classified information:

[F]or all the successes we have had and the advances we have made, serious and unnecessary damage has been caused by media leaks. Unauthorized disclosure of classified information threatens the survivability of the sources and methods that we depend upon. We have lost opportunity, if not capability, because of irresponsible leaks and this has made it easier for our enemies.

Hearing Before the Senate Select Committee on Intelligence: Current and Projected National Security Threats to the United States, S. Hrg. 109-363, p. 5 (March 17, 2005).⁶

In cases of unauthorized disclosure of NDI to the media, the government need not show there was actual harm to the national security from the defendant’s unauthorized disclosure to meet its burden of showing the information was, in fact, NDI; rather, the government must show there was the *potential* for harm to the national security. *See, e.g., United States v. Morison*, 844 F.2d 1057, 1071 (4th Cir.1988). Here, however, the government can show actual harm. *See Gov’t Class’d Add.* As laid out in the classified declaration appended to the Government’s Classified

⁵ Available at <https://www.govinfo.gov/content/pkg/CHRG-107shrg82338/html/CHRG-107shrg82338.htm>.

⁶ Available at <https://www.govinfo.gov/content/pkg/CHRG-109shrg27088/html/CHRG-109shrg27088.htm>.

Addendum, the defendant's choice to betray his oath to his country had real consequences and caused actual harm to the safety of this country and its citizens. *See* Class'd Ex. 6.

In addition to the illegal disclosures to the media, the defendant was also passing classified NDI to a foreign consultant, Consultant 1, without authorization. Over the course of over 20 months, the defendant passed classified NDI to Consultant 1 on at least two occasions. SOF at ¶ 26. The classified NDI related to counterterrorism intelligence the defendant was privy to because of his role as an intelligence analyst and the trust the government placed in him in that role. *See* Class'd Gov. Add. During one exchange, after the defendant told Consultant 1 he had seen footage of a certain event, Consultant 1 joked "unclassified? LMAO." The defendant replied "Hahah good try." *See* Redacted February 2019 Messages (Ex. D); Classified February 2019 Messages (Class'd Ex. 9). In a separate exchange, Consultant 1 confirmed he had received valuable information from the defendant in the past:

Frese: Nothing from our field guys yet, annoyingly.

Re: [redacted] that's interesting. I want to know more haha, but I want to be able to give you something good in return. I've been the lucky one in this exchange my friend.

Consultant 1: You've been very helpful more than once bro.

See Redacted August 2019 Consultant 1 Exchange (Ex. E); *see also* Classified August 2019 Messages (Class'd Ex. 10). These sample exchanges show an ongoing relationship in which the defendant was trading U.S. government information with a foreign national. The tone of the conversations show the defendant's complete nonchalance in compromising information he was only privy to because of the trust placed in him as a clearance holder.

The defendant may argue that, in passing classified NDI to Consultant 1, he strategically chose NDI he knew was to be made public imminently. That attempt at minimization fails in light

of the regimented rules for the classification and declassification of government information. *See* Executive Order No. 13526,⁷ “Classified National Security Information.” The current classification system is an executive function, governed by Executive Order No. 13526, 75 Fed. Reg. 707 (Dec. 29, 2009), which “prescribes a uniform system for classifying, safeguarding, and declassifying national security information.” *United States v. Morison*, 844 F.2d 1057, 1074 (4th Cir. 1988). Executive Order 13526 describes the policies and procedures by which information essential to the nation’s security and foreign relations is protected from unauthorized use, dissemination, handling and storage. Pursuant to that Executive Order, *only* an Original Classification Authority (“OCA”) may classify or declassify national security information. Executive Order 13526 at Sec. 1.3; *cf. El-Masri v. United States*, 479 F.3d 296, 305 (4th Cir. 2007) (quoting *United States v. Marchetti*, 466 F.2d 1309, 1318 (4th Cir. 1972)) (“[T]he courts, of course, are ill-equipped to become sufficiently steeped in foreign intelligence matters to serve effectively in the review of secrecy classifications”); *United States v. Smith*, 750 F.2d 1215, 1217 (4th Cir. 1984) (“[T]he government . . . may determine what information is classified. A defendant cannot challenge this classification. A court cannot question it.”); *United States v. Kiriakou*, 1:12-cr-00127-LMB, Dkt. 62 (E.D. Va. Aug. 8, 2012) (“[T]he classification system is the purview of the executive branch[.]”) (citation omitted). This is because an OCA makes determinations as to what is classified, and what may safely be declassified and disseminated outside the government, based on his or her unique position of access to this country’s full intelligence holdings. *See* DIA Decl. at ¶ 3(c) (Class’d Ex. 11). Individual intelligence analysts are not privy to this important, broader picture. *Id.*

The defendant is not and has never been an OCA. While he may have believed himself an

⁷ Available at <https://www.archives.gov/isoo/policy-documents/cnsi-eo.html>.

expert on certain topics based on the snapshot of information he reviewed, the defendant did not have access to the broader information OCAs digest in order to properly assess the risk of harm from the disclosure of specific national security information. The fact that the defendant believed the NDI he passed to Consultant 1 would imminently become public does not justify his behavior. The defendant was not part of or privy to the high-level decisions as to operations on the ground or how and when NDI would be released. As the defendant himself knew from his extensive training, even where an event on the ground has actually occurred and is, thus, known to the public, certain aspects of the United States government's interest in the event may remain classified. *See id.* at ¶ 6. Release of such classified NDI could alert our adversaries to our country's operational priorities and collection abilities. Such unauthorized disclosures jeopardize theUSIC's ability to collect intelligence and thereby increase risks for our troops on the ground. *Id.* The defendant's decision to disclose NDI to Consultant 1 was not his to make. In making the unauthorized disclosures to Consultant 1, the defendant not only disregarded his extensive training, he created real risk for this country and its citizens.

3. *Need to Reflect Seriousness of Offense and Deter Future Criminal Conduct*

As this Court noted at the defendant's change of plea hearing, this particular crime is one for which general deterrence is of the utmost importance. Clearance holders – those trusted with the most sensitive secrets of our country's defense apparatus – need to understand that the government will find, prosecute, and punish those who violate the trust placed in them. As the Department of Justice has made public in response to Freedom of Information Act ("FOIA") requests, recent years have seen an uptick in the number of media leak referrals from United States Intelligence Community ("USIC") agencies. *See, e.g.,* Steven Aftergood, *Secrecy News*, Federation of American Scientists (Apr. 8, 2019) (44 referrals to DOJ of classified leaks in 2009

vs. 120 in 2017).⁸ The USIC makes such referrals after recognizing its information in open source media publications. Given this increase in volume of media leak investigation referrals, sentences need to reflect the seriousness of the conduct – jeopardizing the very safety of the American people – in order to deter clearance holders who might entertain passing classified NDI to members of the media or others not authorized to receive it. Accordingly, general deterrence counsels in favor of a 108-month sentence.

The specific facts of this defendant’s conduct are particularly egregious. The defendant was passing classified NDI to the media, regularly and unceasingly, over the course of well over a year. And there was no end in sight. In fact, as noted above, for the September 24, 2019 telephonic transmission of NDI to Journalist 2, recorded pursuant to a Title III wiretap, the defendant, not the journalist, initiated the contact. *See* Sept. 24, 2019 Text Message (Ex. B). Further, on that September 24, 2019 call, the defendant raised a new topic with Journalist 2, showing that he was not only taking taskings from the journalists, but also affirmatively shopping new sensitive NDI to them unbidden. *See* Redacted Sept. 24, 2019 Call Tr. (Ex. C); *see also* Classified Sept. 24, 2019 Call Tr. (Class’d Ex. 2).

4. *Avoidance of unwarranted sentencing disparities*

A final sentencing factor to consider is the “need to avoid unwarranted sentencing disparities among defendants with similar records who have been found guilty of similar conduct.” 18 U.S.C. § 3553(a)(6). It is difficult to make comparisons to other cases involving unauthorized disclosures of classified NDI to the media, however, because there have been few such cases prosecuted in federal courts. The issues presented by trying a case involving classified information are complex; and their final resolution, whether by the trial court or on appeal, is uniquely difficult

⁸ Available at <https://fas.org/blogs/secrecy/2019/04/leaks-surge/>.

to predict. *See Kiriakou Sentencing Tr.*, Case No. 12-cr-00127-LMB, 20:23-21:3 [Dkt. 130] (“I recognize the difficulty the government has in prosecuting these types of cases. They have to balance the potential danger of disclosure of very sensitive information when deciding how to proceed[.]”); *see also United States v. Kim*, 808 F. Supp. 2d 44, 55 (D.D.C. 2011) (observing that there has been a “dearth of prosecutions” under Section 793(d) “most likely” because of the “difficulty in establishing such a violation, combined with the sensitive nature of classified information and the procedures that must be followed in using such information in trial”). An adverse determination concerning the handling of classified information at trial can severely hamper, if not end, a § 793 prosecution.

This Court has presided over two such prosecutions – both involving disclosures that occurred over a decade ago. *See Indictment, United States v. Sterling*, Case No. 1:10-cr-00485-LMB [Dkt. 1] (charging passage of classified NDI occurring from 2003 into 2006); *Indictment, United States v. Kiriakou*, Case No. 12-cr-00127-LMB [Dkt. 22] (charging passage of classified NDI occurring in 2008 and 2009). In *Sterling*, the defendant was sentenced to 42 months’ imprisonment following a trial and conviction by a jury. *See Sterling Sentencing Tr.*, Case No. 1:10--cr-00485-LMB [Dkt. 475], at 26:5-7. The *Kiriakou* prosecution ended with the parties entering a plea agreement with a binding agreed-upon sentence of 30 months pursuant to Federal Rule of Criminal Procedure 11(c)(1)(C). *See Kiriakou Sentencing Tr.*, Case No. 12-cr-00127-LMB, 20-21 [Dkt. 130]. This Court has previously commented on the insufficiency of *Kiriakou*’s 30-month sentence, stating during the *Sterling* sentencing:

I also said during [the *Kiriakou*] sentencing that I was troubled by the fact that the identity of an agent was disclosed, and had I not agreed -- and I did agree for the various reasons that we often have in these types of cases where you’re balancing the disclosure problems that the government has against being able to have the case go forward -- I would have probably sentenced him higher, because there is in my view no more critical secret than the secret of those people who are working on

behalf of the United States government in covert capacities, even more than the program itself.

Sterling Sentencing Tr. at 24:8-18; *see also Kiriakou* Sentencing Tr. at 21:3-6 (“I think 30 months is, frankly, way too light because the message has to be sent to every covert agent that when you leave the agency, you can’t just start all of a sudden revealing the names of the people with whom you worked.”).

Times have changed significantly since the *Sterling* and *Kiriakou* prosecutions. The term social media had yet to become part of the mainstream vernacular when *Sterling* and *Kiriakou* were breaking their oaths to the United States. Facebook was not even launched until a year into the charged conduct in *Sterling*. *See This Day in History: February 4, 2004* (launch of Facebook.)⁹ Now, conversely, Facebook is joined by a multitude of online platforms, all able to transmit information around the globe in seconds. Articles “go viral” in a way that could scarcely have been dreamed of in 2003. In fact, the defendant here utilized Twitter’s direct messaging feature to communicate with both Journalist 1 and Consultant 1 as part of his ongoing disclosure of classified NDI to both. The defendant also “retweeted” links to Journalist 1’s articles containing classified NDI, thus assisting in further dissemination of the unauthorized disclosure of our nation’s secrets.

In addition to the advent of social media, most mainstream media outlets now include all of their print content on their websites, allowing instantaneous access to users all over the world, often at no cost. Thus, our foreign adversaries need not even go to the trouble of tasking someone to purchase a physical newspaper to be able to mine our news outlets for NDI. Perhaps this collision of online media content and social media is in part to blame for the notable uptick in

⁹ Available at <https://www.history.com/this-day-in-history/facebook-launches-mark-zuckerberg>.

media leak investigation referrals to the Department of Justice since the *Sterling* and *Kiriakou* prosecutions. The fact is, in 2017 there were 120 media leak referrals to the Department of Justice, compared to 44 in 2009. *See* Secrecy News.¹⁰ While 2018 saw a dramatic drop in that number, the 2018 figure was still double that of the 2009 number. *Id.* In a time when illicit passage of NDI is all too easy, sentences for this conduct need to reflect the seriousness of the betrayal to the American people in order to serve as effective deterrence to would-be leakers.

Given the changes to the nature of media and disclosures since the *Sterling* and *Kiriakou* cases, more recent prosecutions serve as better markers as to sentencing here. In 2017, Reality Winner was charged with a single count of willful retention and transmission of NDI classified at the TOP SECRET level to an online news outlet. *See* Indictment, *United States v. Winner*, Case No. 1:17-cr-00034-JRH-BKE [Dkt. 13]. Winner was accused of and pleaded guilty to transmitting a single TOP SECRET intelligence report on a single occasion to an online media outlet. *Id.* at Dkt. 324 (*Winner* Plea Agreement). Pursuant to Federal Rule of Criminal Procedure 11(c)(1)(C) the Winner plea agreement included an agreed-upon sentence of 63 months' imprisonment. *Id.* at Dkt. 327 (*Winner* Judgment).

Just a few months after the *Winner* sentence, a district court sentenced former Federal Bureau of Investigation ("FBI") employee Terry Albury to 48 months' imprisonment for passage of NDI classified at the SECRET level to a media outlet. *See* Government's Position on Sentencing, *United States v. Albury*, Case No. 0:18-cr-00067-WMW, p. 5 (D. Minn. Oct. 4, 2018) (base offense level of 24 based on transmission of tangible SECRET NDI) [Dkt. 35]. Albury admitted to unlawfully retaining certain documents containing NDI over the course of an 18-month period and passing two of those documents to an online media outlet. *Id.* at Dkt. 1 (*Albury*

¹⁰ Available at <https://fas.org/blogs/secrecy/2019/04/leaks-surge/>.

Information); *see also id.* at Dkt. 16 (*Albury* Plea Agreement).

While the defendant is not charged with the unlawful retention of classified information, sentences in those cases also provide a useful benchmark here. Sentences in retention cases also vary. Nonetheless, significant sentences in those cases, where the defendants were not accused of disclosing any NDI, but rather, of simply improperly retaining such information, bear noting. *See United States v. Ford*, 288 F. App'x 54, 60-61 (4th Cir. 2008) (affirming 72-month sentence for retention of materials classified as Top Secret); *United States v. Martin*, 1:17-cr-00069-RDB (D. Md. 2019) (plea pursuant to Fed. R. Crim. P. 11(c)(1)(C) to 108 months of imprisonment for unlawful retention of materials classified as Top Secret); *United States v. Pho*, 1:17-cr-00631 (D. Md. 2018) (sentence of 66 months for unlawful retention of materials classified as Top Secret); *United States v. Marshall*, 3:17-cr-1 (S.D. TX 2018) (sentence of 41 months for unlawful retention of materials classified at the Secret level). Given the sentences in these cases for individuals convicted of retaining classified NDI, with no further allegation of any dissemination of such information to any unauthorized person, a sentence here of 108 months is appropriate.

No disclosure of classified NDI to the media can be characterized as minor. All such disclosures jeopardize the safety of this country and its people. The defendant's disclosures in this case, however, are particularly egregious, even compared to other such violations of the public trust. Albury received a 48-month sentence for the transmission of SECRET documents. Winner received a 63-month sentence for a single transmission of a TOP SECRET document. Here, the defendant himself admits to transmitting TOP SECRET information to Journalist 1 on 12 separate occasions. SOF at ¶ 13; PSR at ¶ 20. The defendant admits he passed SECRET information to Journalist 1 on another four occasions.¹¹ *Id.* This is in addition to the defendant's transmission of

¹¹ The government's analysis of the dates and times of defendant's telephone calls with Journalist 1 and Journalist 2, along with the accessing of certain classified reporting, cross-referenced against the timing of Journalist 1's

classified NDI to Consultant 1 on multiple occasions and passage of NDI to Journalist 2 on September 24, 2019. SOF at ¶¶ 21, 25; PSR at ¶¶ 28, 31. And there is no indication the defendant would have ever stopped serving as a source of classified information had the FBI not disrupted his efforts.

In addition to transmitting classified NDI, the defendant also confirmed that NDI that Journalist 1 had received from other sources was accurate. SOF at ¶ 20; PSR at ¶ 27. The defendant also admitted to running searches on classified government systems based on specific requests from the journalists. SOF at ¶ 19; PSR at ¶ 26. Perhaps most egregious, the September 24, 2019 wiretap interceptions show that the defendant affirmatively reached out to Journalist 2 to present her with classified NDI on a topic she had not previously asked about. SOF at ¶ 21; PSR at ¶ 28; *see also* Sept. 24, 2019 Text Message (Ex. B); Redacted Sept. 24, 2019 Call Transcript (Ex. C); Classified Sept. 24, 2019 Transcript (Class'd Ex. 8). Thus, the defendant was not simply being lulled into passing classified NDI. The defendant was choosing to approach a member of the media with information he knew to be classified at the SECRET level; information he knew could reasonably be expected to cause serious harm to the national security of this country if made public. *See* SOF at ¶¶ 3, 21; PSR at ¶¶ 10, 28.

In sum, given the gravity and extent of the defendant's disclosures, the defendant's sentence should well-exceed Albury's 48 months of imprisonment and Winner's 63 months. A sentence of 108 months' imprisonment appropriately reflects the seriousness of the criminal conduct here and avoids disparities across sentences for violations of 18 U.S.C. § 793.

publication of the same classified NDI the defendant had viewed on classified government systems, support the inference that the instances of the defendant's passage of NDI are even higher than the numbers agreed to in the Statement of Facts.

III. CONCLUSION

For the foregoing reasons, the government respectfully requests that this Court sentence the defendant to 108 months' imprisonment. A nine-year sentence not only comports with the USSG calculation, but also appropriately reflects the seriousness of the offense and the exceptionally grave risk of harm the defendant created for this country and its citizens.

Dated: June 11, 2020

Respectfully submitted,

G. Zachary Terwilliger
United States Attorney

By: /s/ Jennifer K. Gellie

Danya E. Atiyeh
W. Neil Hammerstrom, Jr.
Assistant United States Attorneys
United States Attorney's Office
2100 Jamieson Avenue
Alexandria, VA 22314
Tel: (703) 299-3700
Fax: (703) 299-3982
danya.atiyeh@usdoj.gov
neil.hammerstrom@usdoj.gov

Jennifer Kennedy Gellie
Trial Attorney
National Security Division
United States Department of Justice
950 Pennsylvania Ave., NW
Washington, D.C. 20530
Tel.: (202) 233-0986
Fax: (202) 233-2146
jennifer.gellie@usdoj.gov

CERTIFICATE OF SERVICE

I hereby certify that on the 11th day of June 2020, I filed the foregoing with the Clerk of the Court using the CM/ECF system, which will send an electronic notification to all counsel of record.

_____/s/
Jennifer Kennedy Gellie
Trial Attorney
National Security Division
U.S. Department of Justice